

Securing Fibre Channel Storage Area Networks

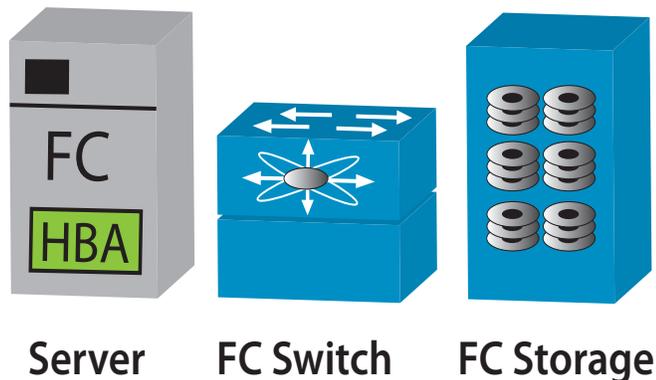
Overview

Storage Area Networks (SANs) are used in government and industry to store large amounts of data while assuring availability and access to that data.

Securing data from accidental or malicious disclosure, whether it is data-in-transit or data-at-rest, is critical to the mission of any organization. SAN security should be carefully considered and then implemented in accord with all applicable security policies.

One important type of SAN is the Fibre Channel (FC) SAN, used for the rapid transfer of data between FC storage devices and between servers and FC storage devices, via FC switches. One or more FC switches in a SAN compose a fabric. Servers have one or more Host Bus Adapters (HBA) that provide a hardware interface to the FC SAN.

This document provides security guidance for FC SAN architectures and is intended for SAN administrators. This security guidance includes critical aspects of access control, authentication, and confidentiality mechanisms.



Access Control

Access control on a SAN can be accomplished by configuring the following in a secure fashion: FC switch ports, zones, Logical Unit Number (LUN) masks, and proprietary access control mechanisms. Before discussing each of these techniques, a discussion of how FC devices and ports are identified is in order, since identity is used in the configuration of SAN access control mechanisms.

Globally unique identifiers, known as World Wide Names (WWN), are used for identification in a SAN. The two types of WWN are the World Wide Node Name (WWNN) and the World Wide Port Name (WWPN). The WWNN applies to SAN devices, while the WWPN applies to ports on a SAN device. The WWN is similar to the Media Access Control (MAC) address used by Ethernet Local Area Network (LAN) devices in that both are intended to be used as globally unique identifiers for interface hardware and both are spoofable.

It is best to control connection requests in as specific terms as possible (i.e. the identity of the connecting port as well as the identity of the connecting device).

- Identify nodes for access control using WWPN + WWNN, or at a minimum, WWPN only.

FC switches are in the core of a SAN. They are the medium through which servers and storage devices communicate to each other. As such, they have physical ports used to interconnect servers, storage devices, and other switches. FC terminology includes the concept of port typing. FC port types



The Information Assurance Mission at NSA

are specified based on different logical modes of operation, and these port types are defined in the FC standards. Both of the following ways to protect switch ports from unauthorized access should be used.

- For each FC switch port, use port locking to associate that switch port with the WWN of the connected device.
- For each FC switch port, use port type locking to restrict the functionality of that port, thereby limiting what type of device can connect to that FC switch port.

A SAN can be divided into sets of one or more servers and one or more storage devices. These sets are known as zones. Zones are created for the purpose of restricting the visibility of portions of a SAN to certain devices. Depending on how zones are implemented, a device that is not a member of a zone may or may not be able to access or communicate with devices in that zone.

Although devices within a zone are only visible to other devices within that zone, devices in a zone are still accessible from outside the zone unless “hard zoning” is used. Hard zones are enforced by FC switch hardware. Physical port numbers on a switch are the best identifier for FC devices in zone configurations. Unlike software-based identifiers (i.e. WWNs), hardware-based identifiers are not susceptible to spoofing.

- Use port number based hard zoning, but if this is not feasible, use WWPN based hard zoning. Push zoning changes to all FC switches immediately.

The data on a FC storage device can be divided into different logical units that are available to servers. The logical units are identified by numbers (LUNs). Since not all LUNs are intended to be available to all servers in the SAN, a means for LUN access control is necessary. This is known as LUN masking.

LUN masks can be created on storage devices, FC switches, or servers, but the ideal place to implement them is where the LUNs are defined, on the storage devices.

- Implement LUN masking on storage devices, but if this is not feasible, implement LUN masking on FC switches.

A Cisco proprietary technique for virtualization that has access control implications is the Virtual SAN (VSAN). While zoning divides a SAN into sets of FC devices, VSANs go a step further by dividing a physical SAN into multiple logical SANs. This is analogous to how a Virtual LAN is used to divide a physical LAN into multiple virtual LANs. A VSAN would include at least one server, at least one switch, and at least one storage device. It would have all the qualities of a SAN and its own instances of SAN services. Zones can be used to further segment a VSAN. Physical port numbers should be used to specify which devices compose a VSAN. The VSAN that is configured this way is referred to as a static VSAN, and static VSANs will help to prevent spoofing.

- When using Cisco FC switches, use static VSANs, but if policy dictates that dynamic VSANs be implemented, they should be WWPN-based.

Authentication

It is important for FC devices to verify the identity of other devices with whom they communicate. Authentication is possible between any FC devices that communicate with each other on the SAN (i.e. servers, switches, and storage devices). Authentication should be performed bi-directionally. This is referred to as mutual authentication.

Three authentication mechanisms available for a FC SAN are: Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP), Fibre Channel Authentication Protocol



(FCAP), and Fibre Channel Password Authentication Protocol (FCPAP). DH-CHAP is a “pre-shared secret” based authentication mechanism. FCAP mutually authenticates FC devices based on digital certificates. FCPAP is based on passwords and uses the Secure Remote Password (SRP) protocol. Security policy should determine which of the three forms of authentication is required.

- Use DH-CHAP, FCAP or FCPAP as specified by local security policy.
- Mutual authentication is preferred over one-way authentication.

Confidentiality

There are two major components of data confidentiality on a SAN. Information should be cryptographically protected in SANs when it is in transit between two FC devices as well as when it is at rest on a FC storage device. Both user data stored on storage devices and SAN fabric data used by FC switches should be protected from unauthorized devices.

To protect data-in-transit, implement Encapsulating Security Payload (ESP) as specified by the Fibre Channel Security Protocols (FC-SP).

- Implement ESP as specified by the FC-SP to encrypt data-in-transit and all communications between FC devices.

To protect data-at-rest, the data should be encrypted before arriving at its destined storage device. This requires the use of special purpose appliances that can encrypt the data that is being sent to a storage device. The placement of these

data-at-rest encryption appliances in the architecture is vendor specific.

- Encrypt data-at-rest on storage devices by using an encryption/decryption appliance.

In addition to protecting user data, information about the SAN should also be protected. The switches in a SAN fabric maintain a synchronized name server database, the purpose of which is to maintain fabric information, including WWN to fabric address mappings. Requests can be made to the name server for fabric information. However, replies containing information on FC devices in a particular zone must only be sent to devices in that zone, or between two zones if those two zones have been configured to allow communication. A request from any other FC device should be considered unauthorized.

- Ignore Name Server requests from unauthorized FC devices.

The switches in a SAN fabric transfer information to each other, and this is referred to as E_Port replication. This transfer happens automatically when a new switch is physically connected to any switch in a fabric. If E_Port replication happens automatically, an unauthorized FC switch or any FC device that appears to be a FC switch can obtain fabric information. Security measures already discussed (e.g. switch-switch mutual authentication, physical port locking) can help restrict automatic E_Port replication.

- Restrict automatic E_Port replication.

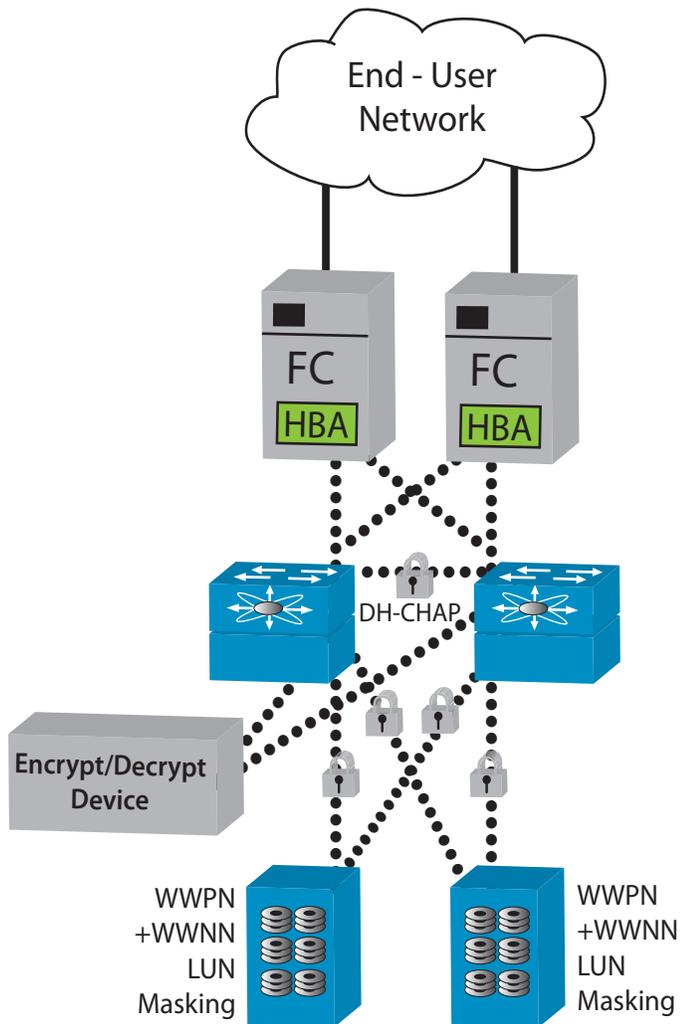
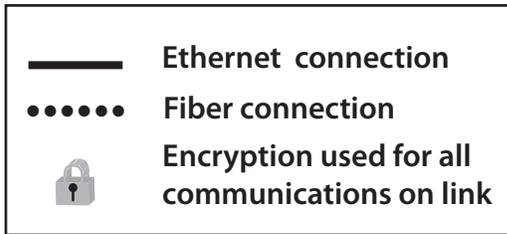


Figure 1: FC SAN with added security

Conclusion

The guidance presented here is intended as an introductory resource to help Fibre Channel Storage Area Network administrators incorporate security into their SANs. It does not claim to be complete guidance or appropriate for all cases. Local security policies should always take precedence over information found within this document. Following the guidance provided in this fact sheet as well as the information found in the document “Best Practices for Storage Networks,” available at Hyperlink “<http://www.nsa.gov/snac>,” will generally enhance the security of Fibre Channel SAN architectures.

Systems and Network Analysis Center (SNAC)

DoD

9800 Savage Rd.

Ft. Meade, MD 20755-6704

410-854-6632

DSN: 244-6632

FAX: 410-854-6604

www.nsa.gov/snac